

**UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY**

**UNITED STATES OF AMERICA**

**v.**

**GEORGE PAYNE**

Crim. No. 07-226 (WJM)

**OPINION**

**HON. WILLIAM J. MARTINI**

**For the United States:**

Dustin Chao  
*Assistant United States Attorney*  
Marc Larkins  
*Assistant United States Attorney*  
United States Attorney's Office  
970 Broad Street  
Newark, NJ 07102

**For the Defendant:**

Denis Kelleher  
Kelleher & Dunne LLP  
17 Battery Place, 11th Floor  
New York, NY 10004

**MARTINI, U.S.D.J.:**

This matter comes before the Court on two pre-trial motions filed by Defendant George Payne, who was charged with receiving child pornography, in violation of 18 U.S.C. §2252A(a)(2)(A), and possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). Following oral argument on August 20,

2007, the Court issued a preliminary ruling from the bench denying Defendant's Motion to Suppress and Motion to Dismiss.

The Defendant subsequently waived his right to a trial by jury. After a bench trial in which the evidence consisted of stipulations jointly submitted by the Defendant and the Government, on October 25, 2007 this Court found the Defendant guilty beyond a reasonable doubt of violating §§ 2252A(a)(2)(A) and 2252A(a)(5)(b).

The Court writes now to supplement its August 20, 2007 ruling from the bench denying Defendant's Motion to Suppress and Motion to Dismiss.

#### **I. MOTION TO SUPPRESS**

On May 3, 2006, Magistrate Judge Madeline Cox Arleo issued a warrant authorizing federal agents to search the Defendant's Hoboken, New Jersey residence for evidence of child pornography. Agents from the United States Immigration and Customs Enforcement ("ICE"), assisted by other law enforcement agents, carried out the search on May 4, 2006. Among other evidence, the agents recovered computer hard drives containing child pornography.

Defendant asks the Court to suppress the evidence recovered during this search of his home, arguing that the search violated his rights under the Fourth

Amendment. The Court begins by reviewing, in detail, the information contained in the search warrant application.

**A. The Search Warrant Application**

The application for the warrant to search Defendant's residence was supported by a signed, sworn statement of ICE Special Agent Craig Funderburk. Agent Funderburk's affidavit provided a detailed discussion of: (1) background information concerning computers and the internet, including how such technologies have affected the nature of child pornography trafficking and possession; (2) the nature of ICE's "New Jersey Investigation" of a commercial website labeling itself "Illegal.CP," which offered access to thousands of images and videos of child pornography via a subscription service; and (3) the evidence establishing that Defendant subscribed to the Illegal.CP website.

*1. Computers and Child Pornography*

In the affidavit, Agent Funderburk, an ICE agent for nearly five years, discussed his training and expertise in investigating crimes involving child pornography, including his participation in executing more than forty search warrants for similar child pornography investigations. (*Aff.* ¶ 1.) Agent Funderburk explained, based upon his training and experience, that computers and the internet have "revolutionized" the methods by which child pornography is produced and disseminated, as well as the methods by which it is accessed and

stored by those who collect it. (*Id.* ¶¶ 1, 10-11.) Agent Funderburk also discussed how computers permit anonymous access to child pornography via subscription- or membership-based websites and enable easy storage of large quantities of child pornography images. (*Id.* ¶¶ 10-11.) Agent Funderburk also explained why the assistance of computer forensic experts is often required to recover images that have been hidden, encrypted or even erased. (*Id.* ¶¶ 10-11, 36-37.)

## 2. *The New Jersey Investigation*

Next, the affidavit provided a broad overview of the New Jersey Investigation into the Illegal.CP website, which began in October 2005. (*Id.* ¶¶ 12-13.) The affidavit discussed how ICE agents discovered a commercial website labeling itself “Illegal.CP,” which offered access to thousands of images and videos of child pornography via subscriptions of 20 and 30 days’ duration. (*Id.* ¶ 13.) Illegal.CP essentially consisted of three components: (1) a banner page advertising child pornography to potential subscribers and urging them to “Join Now,” accompanied by an application page, which appeared after clicking on “Join Now,” and which requests personal and credit card information for the creation of a subscription; and (2) a login page, where approved subscribers could enter a login and password to gain access to the contents of Illegal.CP; and (3) the Illegal.CP website itself, which provided thousands of images and videos of child pornography. (*Id.* ¶¶ 12-17.)

According to the affidavit, the banner page was located at the Uniform Resource Locator (“URL”) of <http://deadundead.info/main.html>. (*Id.* ¶ 14.) The banner page labeled itself “Illegal.CP” and served as an advertisement and a gateway to the subscription-only portions of the Illegal.CP site. (*Id.*) The banner page, which did not require the entry of any personal information, contained approximately one dozen images of minors engaged in sexual acts and proclaimed “[n]ow you are in [sic] few minutes away from the best children porn site on the net!” and “[i]f you join this site you will get tons of uncensored forbidden pics (over 5 at this moment), forbidden stories, and of course, many videos.” (*Id.*) When a user clicked on “Join Now,” he was brought to an application page requesting personal and credit card information. (*Id.*) This page was also part of the <http://deadundead.info> website. (*Id.* ¶ 14 n.4.)

The affidavit also details how an undercover ICE agent purchased access to the Illegal.CP site in October 2005. (*Id.* ¶¶ 15-16.) On October 26, 2005, the undercover agent entered his personal and credit card information into the site, and subsequently received an e-mail from [theodore\\_dykstra@hotmail.com](mailto:theodore_dykstra@hotmail.com) (the “Dykstra account”) with a login and password, as well as a notification that \$79.99 would be charged to his credit card under the name “ADSOFT.” (*Id.*) The agent entered his login and password, and was connected to a site containing thousands of child pornography images. (*Id.* ¶¶ 16-17.) The site was located at the URL of

<http://hualama.cjb.net>. (*Id.* ¶¶ 14, 16.) At the top of the initial page which appeared upon entry into the site was the following message:

FAQ, Please read. "Our site is considered illegal in all countries....Even if you ever have problems with police, you can always say that someone had stolen the information from your credit card and used it. It is very difficult to establish that you were the person to pay."

(*Id.* ¶ 16.) ICE agents examined the contents of the website, and determined that it contained thousands of images of what appeared to be child pornography. (*Id.* ¶ 17.) The website also contained videos, and offered the purchase of additional videos through the website. (*Id.*) The affidavit described three of the still child pornography images in graphic detail. (*Id.*)

The affidavit describes how law enforcement agents then determined that the Internet Protocol ("IP") address for the Illegal.CP website was associated with a server based in Orlando, Florida, which hosted the content of the Illegal.CP site during October and November 2005. (*Id.* ¶ 18.) After confirming the ownership of the server by HostDime.com, ICE obtained a search warrant and searched the server on or about November 17, 2005. (*Id.* ¶¶ 18-19.) A review of the contents of the server revealed the presence of thousands of images and videos of child pornography. (*Id.* ¶ 19.) It also revealed the IP addresses for all contacts with the server between November 9, 2005 and November 17, 2005, demonstrating that hundreds of IP addresses presumably associated with individual subscribers had

visited the Illegal.CP site during that time period. (*Id.*) The data also showed which individual images had been accessed by each IP address. (*Id.*) Two additional search warrants were executed on the server on or about December 14, 2005 and January 5, 2006, both of which yielded additional log files documenting contacts from specific IP addresses with particular images found on the Illegal.CP website. (*Id.*) The affidavit states that ICE believed the location of the server shifted during November and December 2005, and that the use of the HostDime.com server was phased out in favor of another server. (*Id.*) The content of the banner page itself was not located on the server containing the contents of the Illegal.CP website, but on another server located in California. (*Id.* ¶ 14 n.5.)

On or about December 23, 2005, this Court signed an order authorizing the interception of electronic communications occurring to and from the Dykstra account. (*Id.* ¶ 20.) Actual interception commenced on December 27, 2005. (*Id.*) Through these e-mail intercepts, the ICE agents were able to determine how subscriptions to Illegal.CP were processed and approved. Specifically, the ICE agents learned that after accessing the banner page and entering one's personal and financial information on the next page, the information entered was transmitted to the Dykstra account. (*Id.*) The Dykstra account then transmitted the information to a third e-mail account (one of a few addresses, including

joe777@mail.ru and admin@sib-games.com), which would verify the information and result in an approval or denial being e-mailed back to the Dykstra account.

(*Id.*) The Dykstra account would then send an e-mail to the applicant congratulating him on joining the site and providing a password, a login, a link to the Illegal.CP site and a notification of the charge incurred. (*Id.*)

After the interception of the Dykstra account e-mails ended on January 25, 2006 pursuant to the terms of this Court's order, this Court signed an order authorizing continuing interception. (*Id.* ¶ 21.) Interception resumed on or about January 27, 2006 and continued through February 25, 2006. (*Id.*) During this time period, hundreds of individuals were granted access to the Illegal.CP site. (*Id.*) Also during this period, ICE determined that the operators of Illegal.CP had shifted the contents of the site to a new server located in McLean, Virginia. (*Id.* ¶ 22.) On or about February 1, 2006, a search of the new server, known as "Hop One," was conducted pursuant to a court-authorized search warrant. (*Id.*) This search revealed that the Hop One server contained thousands of images and videos of child pornography from the Illegal.CP website, in addition to numerous log files dating from October 2005 through February 1, 2006 which documented contact with the server by numerous IP addresses. (*Id.*) The log files also included data on various subscribers to the Illegal.CP website, including each subscriber's ID, login, e-mail address, IP address and the date and time when the subscription

began. (*Id.*) For each particular video or image accessed by a member, the log files indicated the member's ID, the IP address of the individual accessing the image and the date and time of access. (*Id.*) A second search warrant was executed on March 2, 2006, which provided log file information from February 1, 2006 to February 7, 2006, at which time ICE believes the content of the site was moved to a third server after a disruption of access to the website which lasted for several days. (*Id.*) The affidavit indicates that to make up for the inconvenience of this disruption in access, the Illegal.CP operators offered its subscribers free access to the site's child pornography archives. (*Id.*)

3. *Information Linking the Defendant to Illegal.CP*

Next, the affidavit details how the ICE agents investigating Illegal.CP came to believe that the Defendant had subscribed to Illegal.CP and that evidence of the receipt and possession of child pornography would be found at the Defendant's Hoboken residence.

On or about February 11, 2006, ICE agents intercepted an e-mail from the Dykstra account to joe777@mail.ru, which contained the Defendant's name; his home address in Hoboken, NJ; his e-mail address of gpayne999@yahoo.com; a credit card number (including the card verification value ("cvv"), the three-digit code that appears on the back); a selected login ("lostsoul20") and password ("14lost"); and the IP address from which the information was submitted,

67.85.0.77. (*Id.* ¶ 24.) Then, on February 12, 2006, an e-mail was sent to the Dykstra account from admin@ad-soft.net indicating approval or disapproval of numerous subscription applications. (*Id.* ¶ 25.) The e-mail indicated, in a code understood to the ICE agents based on their ongoing surveillance of the Dykstra account, that the subscription for gpayne999@yahoo.com should be approved. (*Id.*) That same day, an e-mail was sent from the Dykstra account to gpayne999@yahoo.com indicating that he had been billed by ADSOFT for \$79.99 and had been granted a twenty-day membership. (*Id.* ¶ 26.) The e-mail included three links to the Illegal.CP site, as well as a login (“lostsoul20”) and password (“14lost”). (*Id.*) The affidavit notes that because log files for the Illegal.CP servers are only available for review through February 7, 2006, ICE agents did not have log files demonstrating that gpayne999@yahoo.com actually accessed images from the Illegal.CP website after he was granted access on or about February 12, 2006. (*Id.* ¶ 26 n.8.)

ICE agents then moved to corroborate the details linking the Defendant to the Dykstra account e-mails and Illegal.CP. On or about February 13, 2006, ICE agents determined that IP address 67.85.0.77 was controlled by Optimum Online. (*Id.* ¶ 29.) Representatives of Optimum Online then confirmed that this IP address was associated with George Payne at the same Hoboken, NJ address contained in the Dykstra e-mail. (*Id.*) Optimum Online also provided the home phone number

listed on Defendant's account. (*Id.*) On or about March 19, 2006, ICE received the subpoenaed billing records for Defendant's Citibank credit card. (*Id.* ¶ 27.) The card had been charged \$79.99 by ADSOFT on Feb. 11, 2006. (*Id.*) The credit card number corresponded with the number which had been linked to the gpayne999@yahoo.com e-mail address in the Dykstra account e-mails.<sup>1</sup> (*Id.*) Defendant's home address on the Citibank account also matched the Hoboken address listed with Optimum Online and contained in the Dykstra account e-mail. (*Id.*) On or about March 22, 2006, representatives of Yahoo! confirmed that gpayne999@yahoo.com was an active Yahoo! account which was registered to George Payne at the same Hoboken address, and was associated with the IP address of 67.85.0.77. (*Id.* ¶ 28.)

ICE then sought further corroboration of Defendant's Hoboken address by checking records of the Department of Motor Vehicles, Public Service Electric & Gas Company and the United States Postal Service, as well as public phone

---

<sup>1</sup> The affidavit explains that the credit card listed on Defendant's credit card bill is slightly different from the one in the Dykstra account e-mails. (*Id.* ¶ 27 n.9.) Representatives of Citibank confirmed that Defendant verbally disputed a March 5, 2006 charge from a merchant named LEGGS. (*Id.*) Because of this dispute, Payne was issued a new card with a new number. (*Id.*) Although Citibank sent Defendant forms to enable him to formally dispute the LEGGS charges, he had not returned the forms as of May 3, 2006. (*Id.*) The affidavit states that according to Citibank representatives, Payne did not dispute the charge to ADSOFT dated February 11, 2006. (*Id.*)

listings, and by performing surveillance to confirm that George Payne was listed as an occupant on the mailbox outside the apartment. (*Id.* ¶¶ 30-34.)

Based upon all of the above information, Magistrate Judge Madeline Cox Arleo issued a warrant on May 3, 2006 authorizing the search of Defendant's apartment for evidence of child pornography.

Defendant now asks the Court to suppress the evidence recovered during the search of his home. He argues that the search violated his rights under the Fourth Amendment because the search warrant (1) was lacking in probable cause, and (2) was based upon stale information. For the reasons discussed herein, the Court disagrees.

## **B. Probable Cause**

In deciding whether to issue a search warrant, the task of a magistrate judge is to make a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). *See also United States v. Shields*, 458 F.3d 269, 277 (3d Cir. 2006). A magistrate's "determination of probable cause should be paid great deference by reviewing courts." *Gates*, 462 U.S. at 236 (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969)). This Court's duty on review

“is simply to ensure that the magistrate had a ‘substantial basis for . . . [concluding]’ that probable cause existed.” *Id.* at 238-39.

Having carefully evaluated the evidence presented in Agent Funderburk’s affidavit, the Court concludes that Judge Arleo had a substantial basis for concluding that probable cause existed. The affidavit outlined the investigation in detail, explaining at length the basis for ICE’s familiarity with the method of subscribing to Illegal.CP. It described the transmission of Defendant’s personal and financial information to the Dykstra account, which agents had verified as the means of initiating a subscription to Illegal.CP. It outlined the agents’ thorough, independent investigation linking the personal and financial details in the Dykstra e-mails to the Defendant and his home address in Hoboken. And, perhaps most tellingly, the affidavit established that the Defendant used his credit card to pay \$79.99 for a twenty-day subscription — a charge the Defendant never disputed, despite contacting his credit card company to challenge a different charge that occurred just a few weeks later. Considering these facts in combination clearly supports a reasonable inference that the Defendant, in fact, subscribed to Illegal.CP. From there, it “neither strains logic nor defies common sense” to conclude that an individual who has paid \$79.99 for a subscription to a child pornography website has done so because he intends to view and download its content. *United States v. Gourde*, 440 F.3d 1065, 1071 (9th Cir. 2006). The fact

that Defendant declined to challenge the \$79.99 charge provides further support for a reasonable inference that Defendant did, in fact, receive what he expected from “ADSOFT.”

Defendant nonetheless contends that the affidavit was inadequate to support a determination of probable cause, for the following reasons.

*1. Evidence of Access and Downloading*

Defendant points out, correctly, that the affidavit failed to allege that he actually accessed Illegal.CP or downloaded any images of child pornography from the website after he was granted access to the site on February 12, 2006.<sup>2</sup>

Defendant argues that the lack of direct evidence of access or downloading undermines Judge Arleo’s probable cause determination.

“[P]robable cause is a fluid concept — turning on the assessment of probabilities in particular factual contexts — not readily, or even usefully, reduced to a neat set of legal rules.” *Gates*, 462 U.S. at 232. The absence of direct evidence of access or downloading in this case is by no means dispositive of the probable cause issue; rather, it is just one factor for this Court to consider in

---

<sup>2</sup> The affidavit indicates that no log files for that time period were available for agents to review. (Aff. ¶ 26 n.8.) The Court notes, therefore, that the lack of log files implicating Defendant does not possess the same logical significance as it might if, for example, log files were available for the relevant time period, and the log files implicated others, but not Defendant. In other words, the lack of log files does not affirmatively demonstrate, as Defendant contends, that Defendant did not access the website. (Def.’s Br. 9.)

determining whether, under the totality of the circumstances, Agent Funderburk's affidavit established a "fair probability" that child pornography would be found at the Defendant's home. *See Shields*, 458 F.3d at 280.

Defendant relies heavily on *United States v. Zimmerman*, 277 F.3d 426 (3d Cir. 2002), contending that *Zimmerman* "unequivocally held that the affidavit must contain facts that the defendant actually possessed child pornography." (Def.'s Br. 8.) Defendant both oversimplifies and misstates the holding of *Zimmerman*. Moreover, a careful evaluation of the facts reveals several important distinctions between *Zimmerman* and the instant case.

In *Zimmerman*, the Defendant was accused of having shown one video clip of adult pornography to a minor six months prior to the execution of a search warrant on his home and home computer. *Id.* at 429-32. The Third Circuit rejected the search warrant, which sought adult and child pornography, finding that the information supporting probable cause to find adult pornography was stale, and that — as the government conceded — there was no probable cause to search for child pornography. *See id.* at 432-34. Thus, because the issue was not contested, the court in *Zimmerman* did not closely examine the central issue in this case — whether the affidavit established probable cause to search for child pornography. In further contrast to the affidavit in *Zimmerman*, the affidavit here focused exclusively on the Defendant's links to child pornography. Finally, in

*Zimmerman*, the court emphasized that “the affidavit did not even suggest” that the defendant had downloaded the adult pornography in question, and that there was thus no indication it would be found in his home. *Id.* at 435. In this case, however, the affidavit contains strong circumstantial evidence demonstrating that the Defendant paid \$79.99 for a subscription to a child pornography website. This evidence supported a reasonable inference that the Defendant — who did not challenge the charge to his credit card, or otherwise attempt to cancel his paid subscription — would have used his subscription to access to Illegal.CP website and download images, and that such images would therefore have been found in the Defendant’s home. *See Gourde*, 440 F.3d at 1070-71 (because defendant’s paid subscription to site containing illegal images manifested a desire to access illegal images, it was reasonable for magistrate to infer that such images would be found on defendant’s computer).

Even absent direct evidence of access or downloading, therefore, this Court concludes that the evidence in the affidavit, viewed as a whole, was sufficient to support a reasonable inference by Judge Arleo that Defendant had in fact accessed child pornography via his subscription.

## 2. *Significance of Subscription*

Defendant also argues that a subscription alone cannot support probable cause because “a person’s mere propinquity to others independently suspected of

criminal activity does not, without more, give rise to probable cause to search that person.” *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Defendant relies upon *United States v. Kunen*, 323 F. Supp. 2d 390 (E.D.N.Y. 2004) (involving “Operation Candyman”), *United States v. Rubio*, 727 F.2d 786 (9th Cir. 1983) (involving the Hell’s Angels organization) and *United States v. Brown*, 951 F.2d 999 (9th Cir. 1991) (involving corrupt police officers), and argues that the focus of probable cause must be individualized, rather than based solely on one’s association with a group. (Def.’s Br. 8-10.) As the Court has discussed at length, however, the affidavit in this case provided ample circumstantial evidence, particularized to this Defendant, which supported a reasonable inference that evidence of a crime would be found in his home. Moreover, this case is distinguishable from *Kunen*, *Rubio* and *Brown* because here, there were no allegations that the group the Defendant sought to join (*i.e.*, Illegal.CP) ostensibly conducted legal activities — rather, the site itself boastfully declared that it provided only the “best” forbidden child pornography on the internet. The Defendant’s personal, paid subscription to a website supplying wholly illegal content clearly went beyond mere group affiliation or propinquity.

Defendant also argues that the affidavits in prior cases arising from the FBI’s 2001 “Operation Candyman” — several of which were later ruled inadequate — provided stronger support for a probable cause finding than the

affidavit in this case. Defendant's arguments are unconvincing. The Third Circuit recently addressed one of the Candyman cases, and discussed the history of Operation Candyman in great detail, in *United States v. Shields*, 458 F.3d 269 (3d Cir. 2006). Without rehashing the lengthy history of Operation Candyman here, this Court notes several significant differences between this case and the Candyman cases. First, there is no suggestion in Agent Funderburk's affidavit that an Illegal.CP subscription offered any legal alternatives for its members. To the contrary, users were warned, upon joining the site, that its content was "considered illegal in all countries," and were advised of a method of evading punishment if confronted by police. A member of the Candyman e-group, on the other hand, could claim that he did not elect to receive any e-mails (which often contained child pornography videos and images), but only participated in chat room discussions. *See Shields*, 458 F.3d at 270-71, 274. Furthermore, participation in the Candyman group was free, *id.* at 270, whereas Illegal.CP was a for-profit website catering to individuals willing to pay a substantial fee, \$79.99, for a time-limited subscription. Finally, while one could join the free Candyman e-group simply by clicking on a "subscribe" link, Defendant could not have undertaken the multi-step process required to join Illegal.CP by accident or with a mere click of a button.

The facts here are more similar to those in *United States v. Gourde*, 440 F.3d 1065 (9th Cir. 2006). In *Gourde*, the defendant subscribed to Lolitagurls.com, a website that charged an automatically-renewing \$19.95 monthly fee for unlimited access to hundreds of child pornography images.<sup>3</sup> *Id.* at 1067-68. By subpoena, agents learned that Gourde had been a subscriber to the site from November 2001 until January 2002, when the FBI shut down the site. *Id.* at 1068. The affidavit in support of the search warrant indicated, among other relevant facts, that Gourde took affirmative steps to join the site, and that he remained a member for over two months, even though he could have canceled at any time. *Id.* Like the Defendant here, Gourde argued that the affidavit lacked sufficient indicia of probable cause because it contained no evidence that he had actually accessed or downloaded child pornography. *Id.* at 1066. In upholding the magistrate's probable cause finding, the court in *Gourde* stated that "[m]embership is both a small step and a giant leap." The court noted that Gourde's status as a paying member of the site "manifested his intention and desire to obtain illegal images," *id.* at 1070, which supported a reasonable inference that Gourde probably had, in fact, viewed or downloaded images, *id.* at 1071. The court concluded that probable cause was supported by a "triad of solid facts"—that the site had illegal

---

<sup>3</sup> According to the affidavit in *Gourde*, Lolitagurls.com contained adult pornography as well, but the site's owner admitted to the FBI that the site was a child pornography website that he operated as a source of income. *Id.* at 1070.

images; that Gourde intended to have and wanted access to these images; and that if he had in fact received or downloaded images, they were almost certainly retrievable from his computer. *Id.*

Here, as in *Gourde*, the affidavit “left little doubt” that the Defendant had “knowingly and willingly, and not involuntar[il]y, unwittingly or even passively,” paid to obtain access to images of child pornography. *See id.* Evaluating the evidence set forth in Agent Funderburk’s affidavit with a common-sense approach, it is clear that the information in the affidavit, as a whole, provided the necessary “fair probability” to further investigate.

### 3. *Consistency of Illegal Content*

Defendant also argues that while the banner page accessed by an agent in October 2005 advertised an illegal child pornography website, the affidavit fails to allege that ICE verified that the banner page contained the same illegal content in February 2006 when Defendant allegedly subscribed to the website. Defendant also points out that the operators of Illegal.CP moved the website around between October 2005 and February 2006, transitioning from the Florida server to the Virginia server around December 2005 before shutting down the site on February 7, 2006 and moving it to a third location. Defendant also notes that the URLs for the banner application page, the application page, the login page and the Illegal.CP website did not contain any overt references to child pornography (such

as, for example, “Lolitagurls.com”) — instead, the pages were located at cryptic addresses like, for example, hualama.cjb.net, deadundead.info/main.html, and mhumbu.badlink.net. Defendant alleges that these missing pieces create doubt as to what was displayed on the banner page in February 2006 when the Defendant is believed to have accessed the site, and argues that the site’s content could have been entirely innocent at the time he accessed it.

In considering Defendant’s arguments, the Court is mindful of the fact that “[a]fter-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review.” *Gates*, 462 U.S. at 236. While the affidavit in this case does not affirmatively demonstrate that the content of the Illegal.CP site and its component pages remained absolutely constant throughout the server changes and moves, probable cause “means ‘fair probability,’ not certainty or even a preponderance of the evidence.” *Gourde*, 440 F.3d at 1069. Moreover, the affidavit does establish that agents were closely monitoring the site’s location and contents from October 2005 to February 2006. Indeed, between October 2005 and February 2006, ICE agents executed several search warrants on the Illegal.CP servers, retrieving log files that contained detailed subscriber information and download histories. In addition, the agents’ monitoring of e-mails in the Dykstra account showed that the method of subscribing to Illegal.CP from December 2005 through January and February 2006 remained relatively constant compared to the

method which originally led the undercover agent to a child pornography site in October 2005. The accompanying \$79.99 charge to ADSOFT also remained constant. Based on the established patterns documented by ICE, common sense dictates at least a “fair probability” that the Defendant’s \$79.99 payment to ADSOFT was payment for a subscription to a child pornography site, rather than for some innocent, mistaken or wholly unrelated purpose. The fact that the Defendant failed to challenge the \$79.99 charge to ADSOFT, even though he did contact his credit card company to challenge a different charge that occurred just a few weeks later, also weighs against an inference that the payment was mistaken. Finally, in describing the e-mail sent to the Defendant from the Dykstra account, the affidavit stated:

The message then provided three links to the “Illegal.CP” site, stating “for entering, use one of the these [sic] urls:  
<http://mhumbu.badlink.net/> . . . <http://pliac.hotfire.net/> . . .  
<http://fargo.sel.to/>.”

(Aff. ¶ 26.) This unequivocal description of the listed URLs as “links to the ‘Illegal.CP’ site” signifies that ICE did, in fact, verify that these cryptic-sounding links were actually links to Illegal.CP.

In this Court’s practical, common-sense assessment, the facts outlined in the affidavit — including the manner in which Defendant’s information was obtained from the Dykstra account, coupled with the fact that he paid \$79.99 in a manner consistent with other subscriptions to Illegal.CP — supported a reasonable

inference not only that Defendant subscribed to Illegal.CP, but that the site was still functioning as a provider of child pornography at the time of Defendant's subscription.

For all of the foregoing reasons, the Court concludes that the information in the affidavit, as a whole, was sufficient to support a reasonable inference by Judge Arleo that Defendant had in fact accessed child pornography via his subscription.

### **C. Stale Information**

Defendant argues that given the passage of nearly three months between the approval of his subscription on February 12, 2006 and the issuance of the search warrant on May 3, 2006, any information supporting probable cause was stale by the time the warrant was issued. While "[a]ge of the information supporting a warrant application is a factor in determining probable cause," age alone does not determine staleness. *United States v. Harvey*, 2 F.3d 1318, 1322 (3d Cir. 1993). Instead, the Court must also examine the nature of the crime and the type of evidence involved. *Id.*

Considering the nature of the suspected crimes in this case weighs against a finding of staleness. Although the affidavit before Judge Arleo did not explicitly state that collectors of child pornography tend to retain their material for long periods of time, the affidavit made clear why the investigating agents believed that offending material was still on Defendant's computer. Moreover, the "collector

profile” has been discussed at length in child pornography cases; this Court may take notice of the fact that individuals who acquire child pornography — particularly those who have paid a substantial sum for it — ordinarily retain it for long periods of time. The Third Circuit has noted that “collectors of child pornography often store their material and rarely discard it.” *Shields*, 458 F.3d at 279 n.7 (citing *Harvey*, 2 F.3d at 1322-23). *See also United States v. Rowell*, No. 06-0074, 2007 U.S Dist. LEXIS 3277, at \*\*8-9 (N.D. Tex. Jan. 5, 2007) (in case involving Illegal.CP, court held that it could “take notice of the fact that . . . individuals who acquire such child pornography ordinarily retain those images for long periods of time” and view them repeatedly); *Gourde*, 440 F.3d at 1072 (discussing “collector profile” and noting that because they have difficulty obtaining images of child pornography, collectors “act like ‘pack rats,’” rarely, if ever, disposing of their illicit materials).

Considering the nature of digital evidence also weighs against a finding of staleness. The affidavit details how computers and the internet have “revolutionized” the methods by which child pornography is accessed and stored by child pornography collectors — specifically, it explains why images are easy to store and difficult to permanently delete, due to the fact that forensic experts can recover images that have been hidden, encrypted or even erased. (*Aff.* ¶¶ 1, 10-11, 36-37.) Under the circumstances presented in this case, therefore, the affidavit

clearly supports an inference that Defendant's computer would retain at least a "digital footprint" of illegal activity less than three months after his subscription commenced. *See Gourde*, 440 F.3d at 1071.

Whether the delay in this case is calculated from the commencement of Defendant's paid subscription on February 12, 2006 or its expiration 20 days later,<sup>4</sup> this delay of less than three months is well within the time frame where courts have rejected staleness challenges in child pornography cases. *See, e.g., Shields*, 458 F.3d at 279 n.7 (delay of nearly nine months would not have supported staleness challenge); *Gourde*, 440 F.3d at 1071 (given the nature of the crime and the "long memory of computers," unlikely that evidence of child pornography would be stale or missing after delay of less than four months); *United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) ("Information a year old is not necessarily stale as a matter of law, especially where child pornography is concerned."); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (given

---

<sup>4</sup> Defendant also suggests that the delay in this case was, in fact, just over six months, counting from October 26, 2005, when the undercover ICE agent first joined and viewed Illegal.CP, to the issuance of the search warrant on May 3, 2006. This argument is unconvincing. As the Court has already discussed at length, the affidavit establishes that ICE was closely monitoring the website's location and contents from October 2005 to February 2006. Therefore, the information ICE had collected about Illegal.CP was not stale in February 2006 when ICE first discovered the Defendant's connection to the website.

the nature of the crime, there was good reason to believe that child pornography images downloaded ten months prior to search would still be present).

Based on the foregoing, it is clear that the evidence in the affidavit was not stale at the time the warrant was issued.

### **C. Good Faith Exception**

Finally, even if the affidavit did not establish probable cause, the executing officers are entitled to the good faith exception to the exclusionary rule set forth in *United States v. Leon*, 468 U.S. 897 (1984). Pursuant to the good faith exception, suppression “is inappropriate when an officer executes a search in objectively reasonable reliance on a warrant’s authority.” *United States v. Williams*, 3 F.3d 69, 74 (3d Cir. 1993). “The test for whether the good faith exception applies is ‘whether a reasonably well trained officer would have known that the search was illegal despite the magistrate’s authorization.’” *United States v. Loy*, 191 F.3d 360, 367 (3d Cir. 1999) (quoting *Leon*, 468 U.S. at 922 n.23).

Under Third Circuit precedent, the mere “fact that an officer executes a search pursuant to a warrant typically suffices to prove that an officer conducted a search in good faith and justifies application of the good faith exception.” *United States v. \$ 92,422.57*, 307 F.3d 137, 146 (3d Cir. 2002) (internal quotation omitted). The Circuit has identified only “four narrow situations,” *id.*, in which suppression is appropriate:

(1) the magistrate issued the warrant in reliance on a deliberately or recklessly false affidavit;

(2) the magistrate abandoned his judicial role and failed to perform his neutral and detached function;

(3) the warrant was based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; or

(4) the warrant was so facially deficient that it failed to particularize the place to be searched or the things to be seized.

*Williams*, 3 F.3d at 74 n.4 (internal citations and quotation omitted). Defendant argues that the warrant in this case was “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable,” again citing *Zimmerman*, which found the good faith exception inapplicable for the same reason. *Zimmerman*, however, is once again inapposite. In *Zimmerman*, the Third Circuit concluded that from the face of the affidavit, “[a]ny ‘reasonably well-trained officer’ would have known that there was marginal evidence at best of adult pornography, evidence which was anything but current, and no evidence whatsoever to support a search for child pornography.” 277 F.3d at 437.

In this matter, however, as the Court has discussed at length, the affidavit focuses exclusively on evidence of the Defendant’s paid subscription to a website dedicated to child pornography, and contains sufficient evidence to warrant a sincerely held and objectively reasonable belief that child pornography would be found in Defendant’s home. This Court cannot conclude that the warrant in this

case so lacked the requisite indicia of probable cause that it was “entirely unreasonable” for an official to believe to the contrary. Therefore, even if the affidavit did not establish probable cause, the executing officers are entitled to the good faith exception to the exclusionary rule.

For all of the foregoing reasons, Defendant’s Motion to Suppress is denied.

## **II. MOTION TO DISMISS**

In his second motion, Defendant argues that this Court should dismiss the Superseding Indictment because the Child Pornography Prevention Act of 1996 (“CPPA”), which he was charged with violating, is facially unconstitutional.

Defendant’s arguments focus on the Supreme Court’s 2002 decision in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002). In *Free Speech Coalition*, the Supreme Court struck down, as overbroad and unconstitutional, two subsections of the CPPA that were part of the statutory definition of “child pornography.” *Id.* at 256, 258. Those provisions were § 2256(8)(B), which prohibited any visual depiction, including a computer-generated image, that “is, or appears to be, of a minor engaging in sexually explicit conduct,” and § 2256(8)(D), which prohibited any sexually explicit image that was “advertised, promoted, presented, described, or distributed in such a manner that conveys the impression” it depicted “a minor engaged in sexually explicit conduct.” *Id.* at 241-42. The Supreme Court held that § 2256(8)(D) was overbroad because it

prohibited any images pandered as child pornography, without reference to their actual content. *Id.* at 257-58. The Supreme Court declared § 2256(8)(B) unconstitutional because it extended the federal prohibition against child pornography to images that appeared to depict minors, but were in fact produced without using any real children. *Id.* at 239, 250-51. Therefore, the Court reasoned, the statute went beyond *New York v. Ferber*, 458 U.S. 747 (1982), “which distinguished child pornography from other sexually explicit speech because of the State’s interest in protecting the children exploited by the production process.” *Id.* at 240. Under *Free Speech Coalition*, “virtual” child pornography — “speech that records no crime and creates no victims by its production” — is protected under the First Amendment. *Id.* at 250, 256.

After *Free Speech Coalition*, in 2003, Congress passed the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act (“PROTECT Act”), which repealed § 2256(8)(D) and amended the definition of child pornography in § 2256(8)(B) to include a visual depiction that “is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct.” Pub. L. No. 108-21, § 502(a)(1), (a)(3); 18 U.S.C. § 2256(8)(B).

In seeking dismissal of the Superseding Indictment in this case, Defendant argues that the PROTECT Act amendments to 18 U.S.C. § 2256(8)(B) fail to

remedy the problems identified in *Free Speech Coalition*, and that in any event the CPPA as a whole is facially unconstitutional because it burdens a substantial amount of protected speech, even if it may be constitutionally applied in particular circumstances. For the reasons that follow, this Court must reject Defendant's arguments.

Defendant focuses on *Free Speech Coalition*'s holding that the CPPA violated the First Amendment to the extent that it prohibited "virtual" child pornography. This case, however, does not involve "virtual" child pornography. Both the Indictment and Superseding Indictment in this matter charged the Defendant with possessing child pornography as defined in § 2256(8)(A), a separate subsection which defines child pornography as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8)(A) (emphasis added). Moreover, in its opposition to Defendant's motion to dismiss, the Government reiterated that it intended to prove at trial that the Defendant possessed child pornography consisting of visual depictions that actually involved the use of a minor, and would not seek any charge or instruction

as to the Defendant possessing images that are digital or computer-generated depictions of minors.

Defendant argues that § 2256(8)(A) also proscribes legal conduct, and thus runs afoul of *Free Speech Coalition*. Defendant takes issue with the fact that a “visual depiction” under § 2256(8)(A) still includes depictions which are “computer-generated” or “produced by electronic, mechanical, or other means,” arguing that this language encompasses the same type of protected, “virtual” images at issue in *Free Speech Coalition*, and is therefore unconstitutionally overbroad. However, the mere fact that an image is computer-generated or produced by electronic means does not make it “virtual” child pornography of the type at issue in *Free Speech Coalition*. If an image’s “production . . . involves the use of a minor engaging in sexually explicit conduct,” as § 2256(8)(A) specifically requires, then the resulting image is actual — not virtual — child pornography. *See Free Speech Coalition*, 535 U.S. at 250-51. As Defendant conceded at oral argument, regulation of traditional child pornography — that which involves the exploitation of actual children — remains constitutionally permissible under the Supreme Court’s decision in *Ferber*. *See* 458 U.S. at 758-59.

Because this case involves § 2256(8)(A) and not § 2256(8)(B), this Court need not address Defendant’s arguments regarding the constitutionality of § 2256(8)(B) as amended by the PROTECT Act unless we could find that §

2256(8)(B) somehow taints, and renders unconstitutional, the entire CPPA.

Although this is precisely the result Defendant advocates, Defendant's arguments are without merit.

The specific subsections of the CPPA under which the Defendant is charged were unaffected by the holding of *Free Speech Coalition*, which was clearly limited to two subsections of the CPPA, §§ 2256(8)(B) and 2256(D). *See Free Speech Coalition*, 535 U.S. at 258 (“For the reasons we have set forth, the prohibitions of §§ 2256(8)(B) and 2256(8)(D) are overbroad and unconstitutional.”); *United States v. Destio*, 153 Fed. Appx. 888, 891-92 (3d Cir. 2005) (argument that the Supreme Court effectively held the entire CPPA unconstitutional “finds no support in the language of *Free Speech Coalition*”); *United States v. Kelly*, 314 F.3d 908, 910-12 (7th Cir. 2003) (“[*Free Speech Coalition* struck] down only the statute’s expanded definition of child pornography to encompass virtual material.”). The Supreme Court did not disturb its longstanding precedent sanctioning Congress’s ban on traditional child pornography, but was instead concerned with the specific portions of the CPPA which proscribed a significant universe of speech that is neither obscene under *Miller v. California*, 413 U.S. 15 (1973) nor child pornography under *Ferber*, 458 U.S. 747 (1982). *See Free Speech Coalition*, 535 U.S. at 240, 256-57; *Kelly*, 314 F.3d at 909, 912. The other sections of the CPPA can therefore be severed and left

intact. *See United States v. Rodriguez-Pacheco*, 475 F.3d 434, 440 (1st Cir. 2007); *United States v. Wyatt*, 64 Fed. Appx. 350, 351 (4th Cir. 2003); *Kelly*, 314 F.3d at 912.

In sum, because the portions of the CPPA under which the Defendant in this case is charged regulate the possession and receipt of traditional child pornography as defined in 18 U.S.C. § 2256(8)(A) — a definition that remains valid after *Free Speech Coalition* — it is irrelevant to this case whether the PROTECT Act's amendments to § 2256(8)(B) are, as Defendant argues, unconstitutional and overbroad to the extent that they encompass materials not involving actual children.

For the foregoing reasons, Defendant's Motion to Dismiss the Superseding Indictment is denied.

### III. CONCLUSION

For the foregoing reasons, Defendant's Motion to Suppress and Motion to Dismiss are **DENIED**. An appropriate Order accompanies this Opinion.

Dated: October 25, 2007

s/William J. Martini  
**William J. Martini, U.S.D.J.**